# UNITED STATES DISTRICT COURT

for the

District of New Mexico ☑



In the Matter of the Search of
*(Briefly describe the property to be searched or identify the person by name and address)*
2006 White Chevrolet Outlander
License Plate KHA 3YG

Case No. 22-MR-862

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachments A-2

located in the _____ District of New Mexico , there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| *Code Section* | *Offense Description* |
|---|---|
| 18 U.S.C. § 1153 | Offenses committed in Indian Country |
| 18 U.S.C. § 113(a)(3) | Assualt with a Dangerous Weapon |
| 18 U.S.C. § 2 | Aiding and Abetting |

The application is based on these facts:

See Attached Affidavit hereby incorporated by reference as if fully restated herein.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

*Applicant's signature*

Lorraine Hardy. Special Agent
*Printed name and title*

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephonically sworn and electronically signed *(specify reliable electronic means)*.

Date: June 3, 2022

*Judge's signature*

City and state: Albuquerque, New Mexico

Laura Fashing, United States Magistrate Judge
*Printed name and title*

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF NEW MEXICO

IN THE MATTER OF THE SEARCH OF:

a. 1201 S BRAMBLE AVE, FARMINGTON, NEW MEXICO 87401;

b. 14 MILES NORTH OF MORGAN LAKE,
c. LOWER FRUITLAND, NEW MEXICO 87416;

d. NATHANIEL BEGAY (YOB 1993);

e. ROSELINDA CLAW (YOB 1982); and

f. 2006 WHITE CHEVROLET OUTLANDER BEARING AZ LICENSE PLATE KHA3YG

MORE FULLY DESCRIBED IN ATTACHMENT A.

Case No. 22-MR-862

**AFFIDAVIT**

I, Lorraine Hardy, being duly sworn, depose and state as follows:

**INTRODUCTION**

1. I am currently serving as an FBI Special Agent assigned to the FBI, Albuquerque Division, Farmington Resident Agency, where I primarily investigate crimes that occur in Indian Country to include homicide, aggravated assault, child sexual assault, kidnapping and rape. I have been with the FBI for approximately 3 years. I have received on the job training from other experienced agents, detectives, Indian Country criminal investigators, and tribal police officers. My investigative training and experience includes, but is not limited to, processing crime scenes, conducting surveillance, interviewing

subjects, targets, and witnesses; writing affidavits for and executing search and arrest warrants; examining cellular telephones; managing confidential human sources and cooperating witnesses/defendants; serving subpoenas; collecting and reviewing evidence; and analyzing public records.

2. The information set forth in this affidavit has been derived from an investigation conducted by the Farmington Resident Agency of the FBI, the Navajo Nation Department of Criminal Investigations (NNDCI), the Navajo Police Department (NPD) and the Farmington Police Department (FPD). During my investigation, I have developed information I believe to be reliable from the following sources:

a. Information provided by the FBI, NNDCI, NPD, FPD, Pretrial Services, Children Youth and Family Services, New Mexico Department of Corrections (DOC), and other law enforcement officials;

b. Results from physical surveillance;

c. Information provided by witnesses; and

d. Records from the FBI National Crime Information Center (NCIC), Navajo Tribal Courts, New Mexico Courts, and the New Mexico Motor Vehicle Division

3. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are sufficient to establish probable cause for the requested warrant.

## RELEVANT STATUTES

4. This investigation concerns alleged violations of the following:

a. Title 18 U.S.C. § 1153 – Offenses committed in Indian Country;

b. Title 18 U.S.C. § 113(a)(3) – Assault with a Dangerous Weapon; and

c. Title 18 U.S.C. § 2 – Aiding and Abetting.

**PROBABLE CAUSE**

6. On April 28, 2022, NPD responded to multiple gun shots fired at an occupied dwelling in Lower Fruitland, New Mexico. Upon arrival of NPD, the subject was identified by witnesses on scene as NATHANIEL BEGAY (herein after referred to as BEGAY), year of birth 1993. BEGAY had since fled the scene. There were three adult victims and five juvenile victims in the residence during the incident. The owner of the residence, victim one (herein after referred to H.S.J.) year of birth 1954, stated BEGAY fired multiple shots at several different times towards his wife, victim two (here in after referred to as N.J.) year of birth 1953, his son victim three (herein after referred to as H.J.) year of birth 1989 and his five grandchildren referenced as follows: victim four (herein after referred to as Z.J.) year of birth 2006, victim five (herein after referred to as L.J) year of birth 2013, victim six (herein after referred to as V. J.) year of birth 2009, victim seven (hereinafter referred to as H.J.J.) year of birth 2012, and victim eight (herein after referred to as S.J.) year of birth 2009).

7. Based on interviews and evidence associated with this incident, NPD determined BEGAY and his girlfriend, ROSELINDA CLAW (hereinafter "CLAW"), YOB 1982, parked their vehicle on the road by H.S.J.'s residence. CLAW was driving a white 2006 Chevrolet Outlander, bearing Arizona license plate KHA3YG (hereinafter the "SUBJECT VEHICLE." Witnesses reported BEGAY was in the passenger seat and CLAW was in the driver's seat of the SUBJECT VEHICLE. BEGAY exited the SUBJECT

VEHICLE and began firing a 9mm handgun and a .45 caliber Glock handgun towards H.S.J.'s residence. BEGAY appeared angry and was yelling for H.J. to come out of the house. BEGAY and H.J. are related. When H.J. exited onto the front porch, BEGAY continued to fire a handgun in H.J.'s direction. H.J. reported hearing bullets whipping past his head. At some point during the incident, V.J. and S.J. exited the residence and also heard bullets whipping by them. Witnesses described the vehicle as a white four door with a load muffler which matches the description of a vehicle registered to CLAW, with license plate number KHA3YG.

8. H.S.J. and N.J. recognized BEGAY's voice. H.S.J., N.J., and S.J. got into a vehicle and drove over to the SUBJECT VEHICLE, parked behind it, in hopes to talk to BEGAY and retrieve a license plate number. H.S.J. exited the vehicle to walk around to the SUBJECT VEHICLE. BEGAY was standing outside the passenger door of the SUBJECT vehicle and walked to the rear of the SUBJECT VEHICLE to meet H.S.J. BEGAY pointed a firearm at H.S.J. and covered the license plate up with the firearm so H.S.J. could not see it. H.S.J. was afraid for his life and retreated to his vehicle. While parked near the SUBJECT VEHCLE, H.S.J. saw CLAW loading a 9 mm handgun with ammunition and handed it to BEGAY.

9. One of the bullets fired struck the residence. The projectile entered through an exterior wall, through interior wall and lodged in the floor of the kitchen. No one was injured during the incident. NPD and NNDIC located and seized approximately thirty 9mm and .45 caliber casings from the area near the road where BEGAY was standing when the shots were fired, and near where the SUBJECT VEHICLE had reportedly parked. The projectile located in the kitchen was also located and seized.

10. Law enforcement conducted an interview with CLAW, who reported BEGAY was using Metro PCS cellular telephone number, 505-614-9492, to contact and discuss the incident with her. CLAW identified her cellular telephone, Metro PCS cellular telephone number 505-408-0235, which was used to contact and discuss the incident with BEGAY. CLAW stated BEGAY threw both the 9mm handgun and the Glock 45 caliber handgun out of the window of the SUBJECT VEHICLE when fleeing the scene of the incident. CLAW provided agents the approximate location of where the handguns may be found, near Road 36 in Lower Fruitland; however, CLAW believed BEGAY would have already returned to retrieve the firearms. A search for the firearms was conducted by agents and neither the 9mm handgun nor the Glock 45 caliber handgun were found. CLAW also stated BEGAY was angry about an incident that happened several days prior involving H.J. and another relative, Witness-1 (hereinafter " P.J.").

11. Law enforcement conducted an interview of H.J., who stated BEGAY did not get along with P.J. and there was past history between them. H.J. believed BEGAY did not like him because he was friends with P.J. Approximately a week prior to the shooting, BEGAY and P.J. got into a physical altercation and the police were called. BEGAY believed P.J. broke the side view mirror off of his truck and physically assaulted P.J. over it.

12. BEGAY provided telephone number, 505-614-9492, as a contact number with Pretrial Services. Pretrial Services confirmed the telephone number, 505-614-9492, was used on multiple occasions to contact and communicate with BEGAY. CLAW provided CYFD her cellular telephone number, 505-408-0235, as a way to contact her.

CLAW regularly responded to CYFD calls and text messages utilizing telephone number, 505-408-0235.

13. The incident under investigation occurred within the exterior boundaries of the Navajo Nation Indian Reservation. BEGAY, CLAW, and the eight victims are enrolled members of the Navajo Nation.

14. I believe the telephones utilized by BEGAY and CLAW may pertain evidence of the aforementioned incident.

**BACKGROUND ON DIGITAL TECHNOLOGY**

15. The term "computer" refers to "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, mobile phones, and devices. *See* 18 U.S.C. § 1030(e)(1).

16. Based on my training and experience, in this current technological era, people carry their cell phones with them wherever they travel. As a result, cell phones often possess evidence of criminal activity. For example, people use their cell phones to communicate with others through telephone calls, text messages, social media applications, and emails. Cell phones will store these communication records and call logs between individuals. Furthermore, electronic data stored on cell phones can show how and when the cellular device and associated cellular service were accessed or used. This timeline information can help investigators understand the chronology of the crime under investigation. Additionally, information stored by the device and/or the wireless provider may indicate the geographic location of the cellular device and user at a particular

time (e.g., historic cell-site location information; location integrated into an image or video sent via text message to include both metadata and the physical location displayed in an image or video). Stored electronic data may also provide relevant insight into the state of mind of the cellular device's owner and/or user as it relates to the offense under investigation. For example, information relating to the cellular device in the possession of a subject may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement). Cell phones can contain text messages sent and received between the suspects and other possible associates.

17. Based on my training and experience, in this current technological era, people carry their cell phones with them wherever they travel. As a result, cell phones often possess evidence of criminal activity. For example, people use their cell phones to communicate with others through telephone calls, text messages, social media applications, and emails. Cell phones will store these communication records and call logs between individuals. Furthermore, electronic data stored on cell phones can show how and when the cellular device and associated cellular service were accessed or used. This timeline information can help investigators understand the chronology of the crime under investigation. Additionally, information stored by the wireless provider may indicate the geographic location of the cellular device and user at a particular time (e.g., historic cell-site location information; location integrated into an image or video sent via text message to include both metadata and the physical location displayed in an image or video). Stored electronic data may also provide relevant insight into the state of mind of

the cellular device's owner and/or user as it relates to the offense under investigation. For example, information relating to the cellular device in the possession of the wireless provider may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement). Cell phones can contain text messages sent and received between the suspects and other possible associates.

18. In my training and experience, individuals who utilize firearms to commit criminal offenses often conceal evidence of their firearms possession in their residences, or residences of relatives, friends, or associates, and areas surrounding their residences, to include, garages, carports, outbuildings, and vehicles parked on or near their property.

**THE TARGET SUBJECTS, SUBJECT PREMISES, and SUBJECT VEHICLE**

19. The target subjects, subject premises, and subject vehicle to be searched are described in the following paragraphs and in Attachment A-1 and Attachment A-2.

20. Target Subject 1: NATHANIEL BEGAY (BEGAY), YOB 1993. BEGAY has nine prior arrests in New Mexico and two felony state charges pending. BEGAY's prior charges include aggravated battery on a household member, abuse of a child, aggravated assault with a deadly weapon, criminal damage to property, resisting and evading an officer, abandonment of a child, and failure to appear.

21. Subject Premises 1 is located at 14 Miles North of Morgan Lake, Lower Fruitland, New Mexico 87401 and may be described as a single-story, double wide trailer, blue in color with white trim. A log pole fence encloses the property with a locked pipe gate at the entrance. I believe BEGAY lives at Subject Premises-1 with his mother, Lorene BEGAY. Surveillance has seen BEGAY at the residence on May, 25, 2022. BEGAY listed

the residence as his physical address on pretrial release documents. Witnesses have observed BEGAY drive to and from the residence frequently.

22. Target Subject 2: ROSELINDA CLAW (CLAW), year of birth 1982. CLAW has thirteen prior arrests in New Mexico. CLAW has convictions for abandonment of a child and aggravated driving under the influence. CLAW was sentenced to eighteen months in the New Mexico Department of Corrections (DOC) and must utilize a lifetime interlock device when driving device.

23. Subject Premises 2 is located at 1201 S Bramble Ave. Farmington, New Mexico 87401 and may be described as a single-story home on a corner lot. The exterior of the residence is tan stucco with a white front door. A chain link fence encloses the property with two unlocked gates leading to the front entrance. The numbers 1201 are posted next to the front door. I believe CLAW resides at Subject Premises 2. Surveillance has observed the SUBJECT VEHICLE parked in the driveway on May 10, 2022. CLAW was also observed entering the residence. CLAW provided the address to CYFD and Law Enforcement as her place of residence for herself and three children as recently as May 9, 2022.

24. The Subject Vehicle: CLAW reported to law enforcement she owned a 2006 white Chevrolet Outlander with Arizona license plate KHA3YG. A check of Arizona motor vehicle division showed the SUBJECT VEHICLE is registered to CLAW. CLAW reported she was driving the SUBJECT VEHICLE on the evening of the incident. CLAW stated the 9mm handgun and the Glock 45 caliber handgun were kept in the back of the SUBJECT VEHICLE, along with the ammunition for the handguns.

**SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS**

25. As described above and in Attachment B, this application seeks permission to search for records that might be found at the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other electronic storage media (including cell phones). Thus, this warrant would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

26. I submit that if a computer or electronic storage medium is found on the SUBJECT PREMISES, there is probable cause to believe the records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge and training, I know that forensic examiners can recover computer files or remnants of such files months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how an individual has used a computer, what the person used it for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that an individual viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

27. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described in the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the premises because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage

medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which the computer created them, although it is possible for a user to later falsify this information.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when someone accessed or used the computer or storage media. For example, as described herein, computers typically contain information that log:

computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records sought, a review team cannot always readily review computer evidence or data in order to pass it along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a person used a computer, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to document illicit activity, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because someone used it as a means of committing the criminal offense. The computer is also likely to be a storage

medium for evidence of crime. From my training, I believe that a computer used to commit a crime of this type may contain evidence of how BEGAY and/or CLAW used the computer; sent or received data; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

28. Based upon my training and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process, which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, website, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures, which are designed to maintain the integrity of the evidence and to

recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted. Further, the examination may employ techniques that would damage or destroy the device, but result in a forensically sound copy of data stored on the device;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened.

Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

29. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

**BIOMETRIC ACCESS TO DEVICES**

30. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

a. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor,

which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

b. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

c. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this Affidavit, I have reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours.

Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. Due to the foregoing, if law enforcement personnel encounter any devices that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, I request permission to: (1) press or swipe the fingers (including thumbs) of BEGAY and/or CLAW to the fingerprint scanner of the devices found at the SUBJECT PREMISES; (2) hold the devices found at the SUBJECT PREMISES in front of the face of BEGAY and/or CLAW and activate the facial recognition feature; and/or (3) hold the devices found at the SUBJECT PREMISES in front of the face of BEGAY and/or CLAW and activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to request that BEGAY and/or CLAW state or otherwise provide the password or any other means that may be used to unlock or access the devices. Moreover, the proposed warrant does not authorize law enforcement to ask BEGAY and/or CLAW to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.

## CONCLUSION

31. Based on the facts set forth in this affidavit, there is probable cause to believe there was a violation of 18 U.S.C. § 1153 - Offenses committed in Indian Country;

18 U.S.C. § 113(a)(3) - Assault with a dangerous weapon, with intent to do bodily harm, and 18 U.S.C. § 2 - Aiding and Abetting (principals), committed by BEGAY and CLAW, and that evidence of such crimes may be found at the Subject Premises-1, Subject Premises-2, the Subject Vehicle, and on the Target Subjects. Therefore, I submit that this affidavit supports probable cause for warrants to search the premises described in Attachment A-1 and Attachment A-2 and seize the items described in Attachment B.

32. Assistant United States Attorney Kyle Nayback has reviewed and approved this application.

33. I swear that this information is true and correct to the best of my knowledge and belief.

L Hardy

Lorraine Hardy, Special Agent
Federal Bureau of Investigation

Electronically SUBSCRIBED and telephonically SWORN to me this 3rd day of June, 2022.

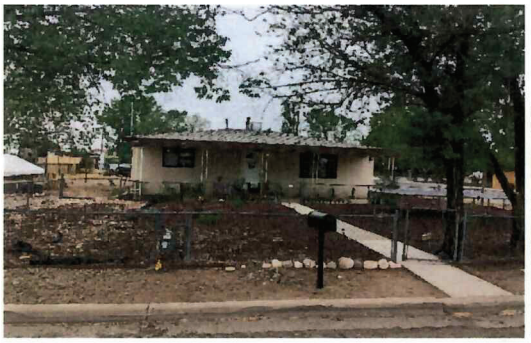
Laura Fashing

HONORABLE LAURA N. FASHING
United States Magistrate Judge

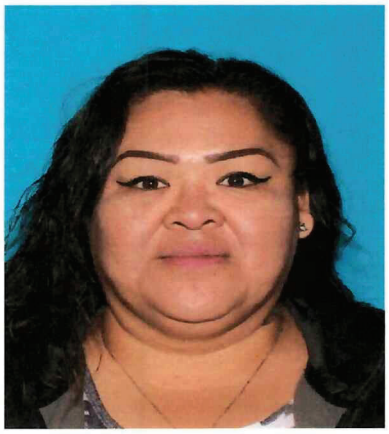
**ATTACHMENT A-2**

The property to be searched is described as follows:

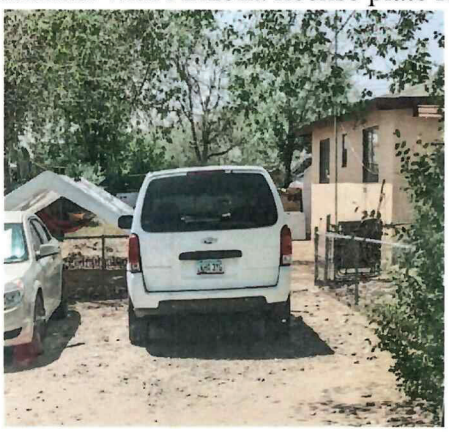
1. The entire property located at 1201 S Bramble Ave. Farmington, New Mexico 87401, including the residential building, any outbuildings, any appurtenances, and the surrounding curtilage ("SUBJECT PREMISES-2"). The property may be described as described as a single-story home on a corner lot. The exterior of the residence is tan stucco with a white front door. A chain link fence encloses the property with two unlocked gates leading to the front entrance. The numbers 1201 are posted next to the front door.




2. The person of Roselinda CLAW, YOB 1982, who appears in the photograph below, provided that this person is located at the subject premises and/or within the District of New Mexico at the time of the search.



3. A 2006 white Chevrolet Outlander with Arizona license plate KHA3YG.



4. During the execution of the search of the premises described in Attachment A, law enforcement personnel are also specifically authorized to compel CLAW to provide biometric features, including pressing fingers (including thumbs) against and/or putting a device in front of a face, or any other security feature requiring biometric recognition, of:
    a. any of the devices found at the premises, and
    b. where the devices are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the devices' security features in order to search the contents as authorized by this warrant.

This warrant does not authorize law enforcement personnel to compel any other individuals found at the premises to provide biometric features, as described in the preceding paragraph, to access or otherwise unlock any device.

This warrant does not authorize law enforcement personnel to require that CLAW state or otherwise provide the password or any other means that may be used to unlock or access the devices, including by identifying the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.

**ATTACHMENT B**

The following items may be seized, which constitute evidence or property designed or intended to use in the commission of a criminal offense, namely violations of 18 U.S.C. §§ 113(a)(3), 1153, and 2 described as assault with a dangerous weapon, with intent to do bodily harm, a crime in Indian country, and aiding and abetting.

1. Firearms and ammunition.
2. All safes or lock boxes, in which firearms and ammunition may be stored for safekeeping against seizure.
3. Records relating to the sale or transfer of 9mm or .45 caliber firearms.
4. 9mm or .45 caliber casings.
5. All electronic storage devices (including: cell phones, "smart" phones, and PDA's capable of sending and receiving images and/or text messages) utilized by BEGAY or CLAW, including cellular telephones with assigned telephone numbers, 505-614-9492 and 505-408-0235.
6. All documents, web history, and communications demonstrating any communication or correspondence with any person discussing the April 28, 2022 shooting.